KEY POINTS ON HIPAA OMNIBUS RULE

1) **Summary**

The Omnibus Final Rule is comprised of the following four final rules:

A) Final modifications to the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:

- Make business associates (BA) of covered entities (CE) directly liable for compliance with certain HIPAA Privacy and Security Rules' requirements.
- Strengthen the limitations on the use and disclosure of protected health information (PHI) for marketing and fundraising purposes, and prohibit the sale of PHI without individual authorization.
- Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
- Require modifications to, and redistribution of, a CE's notice of privacy practices (NPP).
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, Interim Final Rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

B) Final Rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil monetary penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

C) Final Rule on Breach Notification for unsecured PHI under the HITECH Act, which replaced the Breach Notification Rule's "harm" threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.

D) Final Rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans

from using or disclosing genetic information for underwriting purposes, which was published as a proposal rule on October 7, 2009.

2) **Unsecured PHI**

- PHI that is not secured through the use of technology or methodology is deemed to be unsecured.
- Must render data unusable, unreadable, or indecipherable.
- Allowed to use any methods that will reasonably and appropriately protect data in motion, data at rest, and data in use.
- The HIPAA Security Standards make the use of encryption in the transmission process an addressable specification rather than a required specification.
- However, organizations should consider using encryption technology for transmitting PHI over the Internet, and in any situation where a risk analysis shows a significant risk that ePHI transmitted by the organization can be accessed by unauthorized entities.
- If an organization chooses not to encrypt according to the US Department of Health and Human Services (HHS) standards and rely on other protection, if a breach occurs, the organization must still adhere to the Breach Notification Rule.
- Encryption keys should be kept on a separate device from the data they encrypt.
- Considered unusable and/or unreadable if it meets the encryption standards laid out by the National Institute of Standards and Technology (NIST), or if the media on which the PHI is stored has been destroyed in an appropriate manner.
- A CE may de-identify PHI (“expert determination method” or “safe harbor method”) by removing, coding, encrypting, or otherwise eliminating or concealing the information that makes such information individually identifiable, and de-identified information is not considered PHI and thus is not governed by the Privacy Standards.

3) **Breach and Breach Notification**

Breach:

Breach notification is presumed necessary in all situations involving the impermissible acquisition, access, use or disclosure of PHI unless the CE or BA can demonstrate that there is a low probability that the PHI has been compromised (or that an exception applies).

- What is PHI?

  PHI is Individually Identifiable Health Information (IIHI), including demographic information collected from an individual, that:

  a) Is created or received by a covered entity;

  b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;

  c) Either identifies the individual or could reasonably be used to identify the individual; and

  d) Is transmitted or maintained in any form or medium.

- Did the breach involve unsecured PHI?

  "Unsecured protected health information" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS website. Electronic PHI that is password protected but not encrypted is still deemed to be "unsecured."

  If no, the breach does not require notification under HIPAA.

- If yes, does an exception apply?

  a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in the further use or disclosure in a manner not permitted by the Rule.

  b) Any inadvertent disclosure by a person who is authorized to access PHI to a CE or BA to another person authorized to access PHI at the same organization or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Rule.

c) A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably be able to retain such information.

- If an exception applies, the breach does not require notification under HIPAA.
- If an exception does not apply, the CE or BA must assess the probability that the PHI has been compromised. To determine if the PHI has been compromised, the CE/BA must undertake a risk assessment that specifically considers at minimum the following four factors:

  a) The nature, extent, type and sensitivity of the PHI involved and the likelihood of re-identification;

  b) The unauthorized person/entity that used or acquired the PHI, including whether they are subject to confidentiality obligations (such as HIPAA, but including others);

  c) Whether the PHI was actually acquired or viewed, or merely subject to the opportunity for such access; and

  d) The extent to which the risk to the PHI was mitigated, including efforts to obtain assurances that the PHI will not be further used or disclosed, and the reliability of such efforts under the circumstances.

- If the risk assessment does not demonstrate that there is a **low probability** that the PHI has been compromised, breach notification (to individuals, HHS, and, in certain instances, the media) is required pursuant to the Breach Notification Rule. The Omnibus Rule clarifies that CEs must notify HHS within sixty **(60)** days of the discovery of a breach affecting more than 500 individuals. CEs are required to notify HHS of a breach affecting fewer than 500 individuals within sixty days after the close of each calendar year.

Notice Requirements:

- A CE shall provide notice to individuals when a breach occurs, but a CE is free to delegate the responsibility to the BA that is responsible for the breach.
- A breach is treated as discovered the first day the breach is known, or by reasonable diligence, should have been known by any workforce member or agent of the CE, so the CE must implement a system of discovery.
- Notice must be sent with no unreasonable delay and no later than 60 days after discovery by the CE.

- Notification must include:

  a) Brief description of what happened;

  b) Date of discovery and date of breach;

  c) Description of the types of PHI involved;

  d) Any steps an individual should take to mitigate harm;

  e) A brief description of what the CE is doing to mitigate; and

  f) Contact procedures for additional information

- Must make notifications in clear easy to understand language and may need to use brail or large print depending on audience.
- Must provide notice in written form to the last known address, and it may be electronic if individuals previously agreed to it.
- If an individual is a minor or an individual lacking mental capacity, notice to the parent, guardian, or personal representative is sufficient.
- If patient is deceased, notice must be sent to last known address of next of kin. Only required to do this if CE knows that individual is deceased and knows the address of next of kin. If no known address, must provide substitute notice.
- Substitute notice must have all the same information as normal notice and must be reasonably calculated to reach the individuals.
- If under 10 individuals, substitute notice can be done through phone, email, or posted on webpage.
- For substitute notice for 10 or more individuals, CE must either have a conspicuous notice on the webpage for 90 days or in the media, and set up a toll-free number for individuals to call.
- In urgent situations, CE may use additional notice such as telephone and email as well as written.
- More than 500 affected individuals at once, must provide notice to major media sources. Intended to supplement but not substitute individual notice.
- The 500 individuals must all be within one state for the notice provisions to kick in. For instance, if 200 were from one state, 200 from another, and 200 from a third, then it would not apply. However, notification to the HHS Secretary would still apply if incident was deemed to be a breach.
- For breaches of 500 or more, notice must be sent to the Secretary of HHS immediately, and immediately being interpreted as when notice is provided to the individuals.

Notification from BAs

- A BA must notify the CE when a suspected breach has occurred pursuant to the reporting requirements noted on their business associate agreement (BAA).
- The CE is the one that must notify the affected individuals unless the responsibility has been delegated to the BA responsible for the breach.
- Same rules apply for when the breach is "discovered," rules of agency, as well as rules of "reasonable diligence."
- If the BA is acting as an agent of the CE, then the 60-day notification begins when the BA discovered the breach.
- If the BA is acting as a regular contractor of the CE, the 60-day notification begins when the BA informs the CE of the breach.

4) **Enforcement Rule**

- Like all HIPAA Rules, it preempts any State law that is contrary to it; however, it does not preempt a State law that is "more stringent."
- The HHS Secretary must formally investigate complaints indicating violations due to willful neglect, and impose civil penalties upon finding said violations. The investigation is triggered if the initial facts show the "possibility" of willful neglect (i.e., no finding of probability is required.
- The HHS Secretary can move directly to a civil penalty without exhausting informal resolution efforts, particularly in cases involving willful neglect.
- The HHS Secretary retains the power to waive a civil penalty in whole or in part.
- CEs and BAs are liable for the acts of their BA agents. The Federal Common Law of Agency is controlling and CEs and BAs need to pay close attention to the amount of control they exercise over a third party with which they have a BAA. What parties call each other is not dispositive; exercise of control is key.
- An organization's history of HIPAA compliance is relevant to the determination of the civil money penalty.
- The 30-day cure period for violations due to willful neglect, and other violations, begins on the date that the entity first acquires actual or constructive knowledge of the violation and will be determined based on evidence that HHS gathers during its investigation.

5) **Privacy Rule**

The Privacy Rule provides individuals with certain rights regarding their PHI and establishes certain limitations on the use and disclosure of such PHI by CEs and their BAs.

Marketing

- Requires authorization for all treatment and health care operations communications where the CE or BA receives financial remuneration for making the communications from a third party whose product or service is being marketed.
- A CE's NPP should be updated accordingly.

Business Associates

- BAs are directly liable for:

  a) Uses and disclosures that violate the HIPAA Privacy Rule or are in breach of the BAA;

  b) Failing to disclose PHI when HHS requires such disclosures in connection with an investigation of the BA's compliance with HIPAA;

  c) Failing to disclose PHI to a CE, an individual, or such individual's designee when required in connection with an individual's request for an electronic copy of his or her PHI in accordance with HIPAA;

  d) Failing to make reasonable efforts to limit disclosure to the minimum necessary; and

  e) Failing to enter into BAAs with subcontractors that use PHI on their behalf.

- A person/entity becomes a BA by definition, and not because there happens to be a BAA in place; therefore, liability attaches immediately when a person/entity "creates, receives, maintains, or transmits" PHI on behalf of a CE.

Authorizations

- Disclosures for treatment, payment and healthcare operations purposes (TPO) do not require an authorization.
- Authorizations are required from individuals for: 1) most uses and disclosures of psychotherapy notes; 2) uses and disclosures for marketing purposes; and 3) uses and disclosures that involve the sale of PHI.
- Authorizations are not required from individuals for: 1) public health activities; 2) research purposes; 3) the sale, transfer, merger or consolidation of all or part of a CE and for related due diligence; 4) services rendered by a BA pursuant to a BAA and at the specific request

of the CE; 5) providing an individual with access to his/her PHI; and 6) other purposes that the HHS Secretary deems necessary and appropriate.

Decedents

- Requires a CE to comply with the requirements of the HIPAA Privacy Rule with regard to PHI of a deceased individual for a period of 50 years following the date of death.
- IIHI of a person who has been deceased for more than 50 years is not PHI.
- CEs can still disclose PHI of decedents for research purposes.
- CEs may disclose information about a decedent to family members and others who were involved in the decedent's care or the payment of such care, provided that the individual who is the subject of such information did not express a contrary preference to the CE prior to his or her death.

Student Disclosures

- A CE is permitted to disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student. Written authorization is no longer required to permit this disclosure.
- CEs will still be required to obtain and document agreement, which may be oral, from a parent, guardian or other person in loco parentis for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor.

Fundraising

- A CE must provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt-out of receiving further fundraising communications.
- If an individual does opt-out, then the individual's choice to opt-out must be treated as a revocation of authorization.
- The opt-out method for an individual may not cause the individual to incur an undue burden or more than minimal cost (e.g., writing a letter would be considered an undue burden).
- A CE may provide individuals who have opted not to receive fundraising communications with a method to reverse the opt-out and begin receiving fundraising communications.
- A CE may not condition treatment based on an individual opting out of fundraising communications.
- A CE's NPP should be updated accordingly.

Notice of Privacy Practice (NPP)

- The Final Rule requires the NPP contain certain statements in the NPP regarding uses and disclosures that require authorizations.
- The Final Rule requires statements: 1) that an individual has a right to opt out of fundraising communications; 2) for health care providers, that an individual has the right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item; and 3) the right of an affected individual to be notified following a breach of unsecured PHI.
- "Material changes" to a NPP require redistribution.

Right to Request a Restriction

- The Privacy Rule allows individuals to request a restriction on a CE's use or disclosure of the individual's PHI, but a CE is not required to agree to such restriction.
- A CE is required to agree to such a request if:

  a) The disclosure would be to a health plan for payment or health care operations purposes;

  b) The disclosure is not otherwise required by law; and

  c) The item or service was paid by the individual out of pocket, or was paid by a third party (other than the health plan) on the individual's behalf.

- Individuals have a new right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service, and CEs will need to employ some method to flag, or make a notation in the medical record, with respect to PHI that has been restricted.
- Disclosures required by law are still permitted.
- The individual and not the CE is required to notify a downstream Health Information Exchange of the restriction.

Access of Individuals to PHI

- When a CE uses or maintains an EHR with respect to PHI of an individual, the individual shall have a right to obtain from the CE a copy of such information in an electronic format, and the individual may direct the CE to transmit such copy directly to the individual's designee, provided that any such choice is clear, conspicuous and specific.

- Any fees imposed by the CE shall not be greater than the CE's labor costs in responding to the request for the copy.
- A CE is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific form that is not readily produced by the CE at the time of the request, provided that the CE is able to provide some form of electronic copy.
- CEs may still require that an individual make his/her request in writing.

6) **Security Rule**

- Applies to PHI that is in electronic form and requires CEs to implement certain administrative, physical, and technical safeguards to protect such electronic PHI.
- The Security Rule applies to BAs.
- Hybrid entities must now include all BA functions within their covered components.